CARLSON LYNCH, LLP
TODD D. CARPENTER (234464)
1350 Columbia Street, Suite 603
San Diego, CA 92101
Tel: 619-762-1910
Fax: 619-756-6991
tcarpenter@carlsonlynch.com

Attorneys for Plaintiffs and the Proposed Class

[Additional counsel listed on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

KELLY WHALEN, S.M., a Minor, By and Through Her Guardian, Tachah Wade, and VICTORIA EDELSTEIN, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

Case No. 4:20-cv-06361-JST

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Kelly Whalen, S.M., a minor, by and through her guardian Tachah Wade, and Victoria Edelstein, individually and on behalf of all others similarly situated, through undersigned counsel, bring this Consolidated Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, against Defendant Facebook, Inc. ("Facebook" or "Defendant"), and allege the following upon information and belief, except as to the allegations within Plaintiffs' personal knowledge. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. SUMMARY OF THE ACTION

1. Facebook, Inc. is a social media conglomerate founded in 2004. It owns its eponymous social networking platform in addition to a host of subsidiaries.

2. Instagram is a photo and video-sharing social networking service that is owned by Facebook, Inc. It was initially released as an application for the iOS mobile operating system in 2010 before being acquired by Facebook in 2012. Since its acquisition by Facebook, Instagram has steadily amassed new users worldwide. In 2019, there were more than approximately 118 million users in the United States alone.

3. Facebook's social media platform offers a multi-faceted approach for users to connect with one another. In addition to sharing photos and videos, Facebook is a social networking service, which allows users to share news articles, create special interest groups, shop, and more. Instagram, on the other hand, is more limited in its scope of use. Its primary features are photo and video sharing, direct messaging, and "stories," which are photos and/or videos that disappear from a user's profile after 24 hours.

4. Facebook holds the largest facial dataset to date, powered by DeepFace, Facebook's deep-learning facial recognition system, which collects information about face geometry.[1] Based on testing, the DeepFace facial recognition system closely approaches human-level accuracy in identifying faces. Unless a user opts out, Facebook scans photos uploaded to the social network in search of faces it recognizes using its DeepFace technology.[2]

5. Earlier this year, Facebook agreed to pay $650 million to settle a class action that accuses the company of illegally harvesting the protected biometrics of users of its Facebook platform. As part of the settlement, Facebook agreed to delete face templates of users that it had created and stored.

6. As set forth below, Facebook also illegally harvests the protected biometrics of users of its Instagram application. In direct violation of Sections 15(b)-(e) of the BIPA, Facebook is actively collecting, storing, disclosing, profiting from, and otherwise using the biometric data of its reportedly more than 100 million Instagram users, which includes millions of Illinois residents, without any written notice or informed written consent.

[1] https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

[2] https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html

7. Facebook has readily admitted to its collection of biometrics from users. As explained by Facebook, its use of face recognition technology includes analyzing uploaded photos and videos it thinks a user may appear in on Facebook, such as a user's profile picture, as well as photos and videos that he/she has been tagged in, and then creates a unique number for that user, called a template.[3]

8. Its facial recognition software works by scanning faces of unnamed people in photos and videos to analyze details of individuals' faces, checking whether they match with those for whom Facebook has already created templates. While Facebook claims that users are in charge of that process, in reality, people cannot actually control the technology because Facebook scans their faces in photos and videos uploaded by *other* users even if their individual facial recognition setting is turned off.[4]

9. Facebook claims it uses an individual's template to find photos and videos a user appears in, to suggest tags, and to provide more relevant content and feature recommendations.[5] Facebook also surreptitiously captures its Instagram users' protected biometrics without their informed consent and, worse yet, without actually informing users of its practice. Upon information and belief, once Facebook captures its Instagram users' protected biometrics, it associates this data with an existing Facebook template and/or includes this data in its dataset of biometrics that it uses to power, train, and develop its facial recognition software. Moreover, it then uses this biometric data for its own business and financial gain, including, but not limited to, bolstering its facial recognition abilities across all of its products, including the Facebook application and sharing this information among various entities. Facebook does all of this without providing any of the required notices or disclosures required by Illinois' BIPA.

10. Plaintiffs bring this action individually and on behalf of a proposed class in order to stop Facebook's violations of the BIPA, and to recover statutory damages for Facebook's unauthorized collection, storage, disclosure, profiting from, and use of their biometric data in violation of the BIPA.

[3] https://www.facebook.com/help/122175507864081
[4] https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html
[5] https://www.facebook.com/help/122175507864081

II. PARTIES

11. Plaintiff Kelly Whalen is, and has been at all relevant times, a resident and citizen of the state of Illinois and a resident of Cook County, Illinois. Ms. Whalen first created an Instagram account on November 17, 2011, and has used Instagram regularly since that time.

12. During the relevant time period, Ms. Whalen accessed Instagram on both her computer and phone to post photographs, view content posted by other users, and react to that content via comments and "likes." Ms. Whalen frequently tagged herself and others in photographs posted on Instagram, and appeared in photographs uploaded by others to Instagram. Ms. Whalen was not aware that any facial recognition data or other biometric data was being collected by Facebook through her Instagram use.

13. Plaintiff S.M., by and through her guardian, Tachah Wade (her mother), is a minor child and a resident and citizen of the state of Illinois and a resident of Kendall County, Illinois. S.M. is the owner of an Instagram account, which includes content she has posted.

14. During the relevant time period, S.M. accessed Instagram on her phone to post photographs, view content posted by other users, and react to that content via comments and "likes." In addition to photographs of herself that she uploaded to her account, S.M. was frequently tagged in photographs uploaded by others to Instagram. S.M. was not aware that any facial recognition data or other biometric data was being collected by Facebook through her Instagram use.

15. Plaintiff Victoria Edelstein is, and has been at all relevant times, a resident and citizen of the state of Illinois and a resident of Lake County, Illinois. Ms. Edelstein first created an Instagram account in 2017 and has used Instagram regularly since that time.

16. During the relevant time period, Ms. Edelstein accessed Instagram on both her computer and phone to post photographs, view content posted by other users, and react to that content via comments and "likes." Ms. Edelstein frequently tagged herself and others in photographs posted on Instagram, and appeared in photographs uploaded by others to Instagram. Ms. Edelstein was not aware that any facial recognition data or other biometric data was being collected by Facebook through her Instagram use.

17. Defendant Facebook is a Delaware corporation with its headquarters and principal executive offices at 1601 Willow Road, Menlo Park, California 94025. Facebook is a citizen of the states of Delaware and California. Facebook is also registered to conduct business in the State of Illinois (file number 66267067) and maintains an office in Cook County, Illinois.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction pursuant to 28 U.S.C. §1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are well in excess of 100 class members. Because it is estimated that the Class will have thousands of members and Defendant's intentional and reckless violations of BIPA are punishable by statutory damages of $5,000 per violation, the amount in controversy is well in excess of $5,000,000. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. §1367.

19. The Court has personal jurisdiction over Defendant because it has affirmatively established and maintained sufficient contacts with California in that Defendant is registered to do business in this State, is headquartered in this State, and conducts significant business in this State.

20. Venue is proper under 28 U.S.C. §1391(b)(1) because Defendant's principal place of business is in this judicial district.

IV. SUBSTANTIVE ALLEGATIONS

I. Biometric Information and the Illinois BIPA

21. A "biometric identifier" (together with "biometric information,"[6] "biometrics" or "biometric data") is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA, facial features, and voice, among others.

22. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically

[6] The BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. Plaintiffs herein use the terms "biometric information" and "biometric identifier" interchangeably.

unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

23. In recognition of this legitimate concern over the security of biometric data, the Illinois Legislature enacted the BIPA, which requires, *inter alia*, that companies in possession of biometric data establish and maintain a satisfactory biometric data retention and deletion policy. Section 15 (a) of the BIPA requires that "[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

24. As set forth more fully herein, Facebook has violated Section 15(a) of the BIPA by failing to develop and make available to the public the requisite retention and deletion plan and, upon information belief, by failing to destroy such biometrics when the purpose for collecting and obtaining the biometrics have been satisfied or within three years of Plaintiffs' and Class Members' last use of the app.

25. Further, BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, ***unless it first***:
>
> ***(1)*** ***informs*** the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> ***(2)*** ***informs*** the subject or the subject's legally authorized representative in writing of the ***specific purpose and length of term*** for which a biometric identifier or biometric information is being collected, stored, and used; ***and***
>
> ***(3)*** receives a ***written release*** executed by the subject of the biometric identifier or biometric information or the subject's legally authorized ***representative***.

740 ILCS 14/15(b).

26. As alleged herein, Facebook's practices of collecting, storing, and using Instagram users' biometric information without informed written consent violates all three prongs of §15(b) of the BIPA.

27. Facebook has also violated Section 15(c) of the BIPA by selling, leasing, trading, or otherwise profiting from a person's biometrics, as set forth more fully below.

28. Facebook has likewise violated Sections 15(d)-(e) of the BIPA by disclosing, redisclosing, or otherwise disseminating the biometrics captured from media uploaded to Instagram, as set forth more fully below.

II. Facebook Collects, Stores, Discloses, Profits from, and Otherwise Uses Plaintiffs and Class Members' Biometric Data in Violation of the BIPA

29. Instagram has over one billion users worldwide and millions of users in Illinois alone.

30. Instagram allows its users to create a personal page where users can upload photographs and videos, participate in live video broadcasts, and communicate and interact with other Instagram users. Approximately 95 million photos are shared on Instagram each day, with over 40 billion photos and videos shared on the platform since its inception.

31. Facebook has employed its facial recognition technology continuously from the time it was first introduced in 2010, including the time period after its acquisition of Instagram in 2012, and continuing to the date of the filing of this Complaint.

32. Facebook's sophisticated facial recognition technology works by collecting and analyzing the facial features of individuals appearing in photographs and videos uploaded to Facebook and generating a "biometric signature" or "face template" of each individual's face that appears therein. This facial template is based on each person's facial geometry and is specific to that person. Facebook, upon information and belief, also collects biometric data from Instagram users. It scans photos, videos, or other content uploaded to Instagram for biometric data. As Facebook's Instagram and Facebook users continue to manually tag friends, family, and other people they recognize in a photograph, Facebook's software automatically compares those images to the face templates and other biometrics in its database. If there is a match, Facebook may identify the user.

33. Facebook is then able to identify the individuals whose biometrics it has captured by cross referencing the biometric data of individuals appearing in Instagram photographs with face templates that it has already linked with an identified individual (for instance, the face template created for the individual by Facebook or companies with whom Facebook shares captured biometrics), and identify the individual when there is a match.

34. Prior to January 1, 2020, Facebook has never informed Instagram users that it collects their biometric data. Rather, the Instagram Data Policy merely states that Facebook collects information "you and others provide" to the app, in the form of both posted content and anything users might see through the camera, and that its systems ***automatically process*** the content and communications provided by users ***to analyze context and what is in them*** (emphasis added).[7]

35. In fact, Facebook actively mislead Instagram users about whether it was collecting facial recognition data. Instagram's Data Policy states, "**If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences**."[8] However, Instagram users have no ability to turn off any facial recognition software within the app. Furthermore, the Instagram Data Policy states, "If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you."[9] As set forth below, these statements are untrue.

36. On January 1, 2020, Facebook published, for the first time, its California Privacy Notice for its California users as a supplement to its current Data Policy in compliance with California's Consumer Privacy Act (CCPA).[10] Instagram admits in this notice that any of the information disclosed within the California Privacy Notice may have been collected from users over the past 12 months. While California is currently the only state requiring these types of disclosures to consumers, the content of the notice demonstrates that Facebook has been collecting biometric data from its Instagram users for, at minimum, the 2019 calendar year. The California Privacy Notice is reproduced in part below (emphasis added):

---

[7] *See* https://help.instagram.com/155833707900388 Section I: What Kinds of Information Do We Collect?
[8] *See* https://help.instagram.com/519522125107875 Section II: How Do We Use This Information?
[9] *Id*.
[10] *See* https://help.instagram.com/2482657248648591 "California Privacy Notice"

Categories of Personal Information we collect may include:	Examples of how Personal Information is used include:	Parties with whom your information may be shared include:
• ***Identifiers***; • Data with special protections, if you choose to provide it; • Commercial information, if you choose to provide it; • ***Photos and face imagery that can be used to create face-recognition templates if you or others choose to provide it and you have the setting turned on.*** • Internet or other electronic network activity information, including content you view or engage with; • Location-related information, including precise device location if you choose to allow us to collect it; • ***Audio or visual Information, including photos and videos, if you or others choose to provide it;*** • Professional or employment information, if you choose to provide it; • Education information, if you choose to provide it; • Financial information, if you choose to provide it; and • Information derived from other Personal Information about you, which could include your preferences, interests, and other information used to personalize your experience.	• Providing, personalizing, and improving our Products; • Facilitating transactions, providing measurement, analytics, advertising, and other business services; • Promoting safety, integrity, and security; • Communicating with you; • Researching and innovating for social good; and • To perform other business purposes.	• People and accounts you share and communicate with; • People and accounts with which others share or reshare content about you; • Apps, websites, and third-party integrations on or using our Products; • New owners in the event of a change of ownership or control of all or part of our Products or their assets changes; • Partners, including partners who use our analytics services, advertisers, measurement partners, partners offering goods and services in our Products, vendors and service providers, and researchers and academics; • Law enforcement or other third parties in connection with legal requests; and • Facebook Companies.

37. Although Facebook's California Privacy Notice indicates that it collects Instagram users' protected biometrics "if you or others choose to provide it and you have the setting turned on,"

Facebook's belated, after-the-fact notice to Instagram users cannot constitute compliance with the BIPA for a variety of reasons, including that Facebook only allowed Plaintiffs and Class Members to opt out *after* it collected their protected biometrics, and even then, only if Plaintiffs and Class Members knew to look for the opt-out option, which, upon information and belief, is not even possible through a user's *Instagram* account.[11]

38. In any event, Instagram users *cannot* opt out. Indeed, Instagram users are not even given an opportunity to provide a written release because Facebook automatically processes content and shares it across its platforms. Rochelle Nadhiri, a Facebook spokeswoman, said its system analyzes faces in users' photos to check whether they match with those who have their facial recognition setting turned on. This means that users can never really "opt out" of Facebook's use of facial recognition. So even if a user does not have facial recognition activated within their personal account, their photo may still be scanned, collected, and entered into Facebook's database if it matches with a user's data who does have the facial recognition setting activated.[12] This also means that one can never truly "opt out" because Facebook must capture and compare the biometrics of a face before learning if that face, in fact, matches with faces of users who have their facial recognition setting turned on or off.

39. Further, Facebook concedes that it collects information such as the location of a photo, Instagram users' current location, where they live, the places they go, and the businesses and people they are near to "provide, personalize and improve our Products." As such, Facebook knows, or should know, that Plaintiffs and Class Members are Illinois users.[13]

40. Moreover, upon information and belief, Facebook disclosed Instagram users' biometric data not only to teams operating across its own various platforms, but also with third parties. Facebook concedes that biometrics harvested from Instagram's photographs and videos may be shared with other apps, websites, and third-party integrations, Facebook's partners, including partners who use Facebook's analytics services, advertisers, measurement partners, partners offering goods and

[11] *See* https://help.instagram.com/519522125107875, directing Instagram users to "opt out" via settings on their *Facebook* profile.
[12] *See* https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html
[13] *See* https://help.instagram.com/155833707900388

services within Facebook's products, vendors and service providers, researchers and academics, law enforcement, and Facebook Companies, including Facebook Payments Inc., Onavo, Facebook Technologies, LLC, Facebook Technologies Ireland Limited, WhatsApp Inc., WhatsApp Ireland Limited, and CrowdTangle (collectively, "Facebook Companies").[14]

41. Facebook and Instagram share infrastructure, systems, and technology with other Facebook Companies and process information about the user across the Facebook Companies.[15] This includes, upon information and belief, using Facebook's facial recognition technology to process biometrics collected from Instagram users, which are then used to enhance already-existing facial templates of those users.

42. For example, Facebook is currently the subject of antitrust litigation in Germany, where it is alleged to have broken competition laws by combining personal data collected about users across its different platforms, including Instagram, to create "super profiles" for users.[16] A ruling from German regulators prohibited Facebook from combining Facebook user account data with user data on company services like WhatsApp and Instagram.[17]

43. Upon information and belief, Facebook's shared infrastructure, systems, and technology and processing of user information across the Facebook Companies includes using the biometrics harvested from its Instagram users' uploaded material to improve the algorithms that power its facial recognition abilities across all of its platforms, including, but not limited to, its Facebook application where, for example, Facebook uses its facial recognition to suggest tags to Facebook users and lets Facebook users know when their photos are uploaded by someone else.[18]

44. Upon information and belief, Facebook also includes the biometrics captured from Instagram users' uploaded material, as well as Instagram users' tagging information, to bolster its databases of biometrics, face templates, and tagging information that enables Facebook's facial recognition to continue learning and improving, which, in turn, enhances all of Facebook's facial

[14] *See* https://help.instagram.com/2482657248648591
[15] *See* https://help.instagram.com/155833707900388 Section IV: How Do the Facebook Companies Work Together?
[16] *See* https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html
[17] *See* https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html
[18] *See* https://www.facebook.com/help/122175507864081 What is the face recognition setting on Facebook and how does it work?

recognition products, including, for example, its predictive tagging feature on the Facebook application.[19] Several of Facebook's products, such as Moments, an application Facebook introduced in 2015, capitalizes on Facebook's facial recognition technology.[20]

45. Several of Facebook's prior patent filings further attest to Facebook's commercial purposes in developing its facial recognition technologies. These patents reportedly described one system that could detect consumers within stores and match those shoppers' faces with their social networking profiles, and another in which cameras near checkout counters could capture shoppers' faces and match them with their social networking profiles.[21]

46. As such, Facebook profits from its use of its Instagram users' protected biometrics by using them to improve the accuracy of its own facial recognition services, to expand the datasets which enable its facial recognition software, and to cement its market-leading position in facial recognition and social media.

47. Accordingly, Facebook and Instagram have collected, captured, or otherwise obtained Instagram users' biometric identifiers or biometric information, as those terms are defined in Section 10 of BIPA, from content that Instagram users uploaded to Instagram.

48. Facebook and Instagram are in possession of Instagram users' biometric identifiers or biometric information from content that Instagram users uploaded to Instagram.

49. Facebook and Instagram scan photographs, videos, or other content uploaded to Instagram for biometric identifiers or biometric information.

50. In direct contravention of Section 15(a) of the BIPA, Facebook has failed to develop and make available to the public its requisite retention and deletion plan and, upon information belief, by has failed to destroy such biometrics when the purpose for collecting and obtaining the biometrics have been satisfied or within three years of Plaintiffs' and Class Members' last use of the app.

---

[19] *See* https://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why#:~:text=Facebook-,Facebook's%20Moments%20app%20uses%20facial%20recognition%20technology%20to%20group%20photos,friends%20who%20are%20in%20them.&text=When%20someone%20tags%20you%20in,reminder%20of%20a%20shared%20memory. (describing the benefit to facial recognition algorithms of additional photographs and tagging information).

[20] *See* https://techcrunch.com/2015/06/15/facial-recogbook/

[21] *See* https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html

51. In direct contravention of §15(b) of the BIPA, Facebook collected Plaintiffs' and Class Members' biometrics without informing them that it would collect, store, and use their biometric facial data, without informing Instagram users of the specific purpose and length of term for which their biometric data would be collected, stored, and used, and without receiving a written release from Instagram users before it began to collect, store, disclose, profit from, and otherwise use their biometric data.

52. In direct contravention of §15(c) of the BIPA, Facebook profited from Plaintiffs' and Class Members' protected biometrics.

53. In direct contravention of §15(d)-(e) of the BIPA, Facebook voluntarily disclosed and otherwise disseminated Plaintiffs' and Class Members' protected biometrics.

III. Plaintiffs and Class Members' Injuries and Damages

54. As alleged herein, as a result of Facebook's unlawful conduct, Plaintiffs and Class Members have already sustained injuries and face many more imminent and certainly impending injuries, which they will continue to suffer.

55. Facebook's unlawful conduct has resulted in, among other injuries: (a) Plaintiffs' and Class Members' unique biometric identifiers and information being collected, captured, obtained, disclosed, and otherwise disseminated without the requisite notice having been given and without the requisite releases having been obtained; and (b) Plaintiffs and Class Members being deprived of the very control over their biometric identifiers and information that the BIPA was designed to protect.

56. To this day, Plaintiffs and Class Members do not know which, or how many, individuals or entities have received, obtained, accessed, stored, disclosed, or otherwise made use of Plaintiffs' and Class Members' biometric identifiers and information, exposing them to the imminent and certainly impending injuries of identity theft, fraud, stalking, surveillance, social engineering, and other invasions of privacy.[22]

57. As a result of Facebook's misconduct, Plaintiffs and Class Members have no recourse for the fact that their biologically unique information has been compromised. Moreover, Plaintiffs

[22] *See* https://www.forbes.com/sites/forbestechcouncil/2018/04/03/facial-recognition-tech-10-views-on-risks-and-rewards/#54d3e1716b3c

and Class Members are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

IV. Plaintiffs' Personal Experiences

58. Ms. Whalen is a resident of Palos Heights, Illinois. Ms. Whalen signed up for an Instagram account in Palos Heights, Illinois in 2011, and has since then uploaded numerous photographs.

59. Since joining Instagram, Ms. Whalen has uploaded and posted many photographs to Facebook's network from Instagram that include images of her face, and Ms. Whalen has tagged herself in many of those photographs. Ms. Whalen's face has also appeared in many photographs that other Instagram users have uploaded to Instagram, and Ms. Whalen's face has been tagged by other Instagram users in many such photographs. Many of these photographs were taken in Illinois and were uploaded to Ms. Whalen's account from her computer in Illinois.

60. S.M. is a resident of Yorkville, Illinois. S.M. signed up for her Instagram account in Yorkville, Illinois.

61. Since joining Instagram, S.M. has posted photographs and videos to Facebook's network from Instagram that include images of her face. She has also been tagged in photographs that other Instagram users have uploaded to Instagram. Many of these photographs were taken in Illinois and were uploaded to S.M.'s account in Illinois.

62. Ms. Edelstein is a resident of Mundelein, Illinois. Ms. Edelstein signed up for an Instagram account in Mundelein, Illinois in 2017, and has since then uploaded numerous photographs.

63. Since joining Instagram, Ms. Edelstein has uploaded and posted many photographs to Facebook's network from Instagram that include images of her face, and Ms. Edelstein has tagged herself in many of those photographs. Ms. Edelstein's face has also appeared in many photographs that other Instagram users have uploaded to Instagram, and Plaintiff's face has been tagged by other Instagram users in many such photographs. Many of these photographs were taken in Illinois and were uploaded from Ms. Edelstein's computer in Illinois.

64. As is the case for Class Members, Facebook has, upon information and belief, captured biometric identifiers and information from Plaintiffs' photographs by automatically locating and

scanning Plaintiffs' faces, and by extracting geometric data relating to the contours of their faces and the distances between their eyes, nose, and ears – data which Facebook then collected and stored, as set forth more fully below.

65. The biometric data collected from Plaintiffs, upon information and belief, was stored and used by Facebook for research purposes to develop its own facial recognition technologies across the various services and products it offers in connection with its Facebook Companies, including its advertising services. Facebook stores, discloses, profits from, and otherwise uses Plaintiffs' biometrics without their knowledge or consent.

66. Plaintiffs did not receive notice that Facebook would collect, store, profit from, disclose, or otherwise use their biometric data when they used the Instagram app.

67. Facebook never sought – and Plaintiffs never provided – informed consent, in writing or otherwise, to Facebook's collection, creation, storage, or use of their biometric data.

68. Plaintiffs accordingly were never provided an opportunity to prohibit or prevent Facebook from collecting, storing, disclosing, profiting from, or otherwise using their protected biometrics.

V. CLASS ACTION ALLEGATIONS

69. Plaintiffs bring this lawsuit on behalf of the following proposed class (the "Class") under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following Class, defined as follows:

> ***All Instagram users living in Illinois who had their biometric information or identifiers, including scans of their face geometry, collected, captured, received or otherwise obtained by Facebook through materials uploaded to the Instagram application.***

70. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint.

71. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint-venturers, or any entities controlled by Defendant, and its heirs, successors, assigns, or

other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's staff and immediate family.

72. ***Numerosity.*** The members of the Class are so numerous that individual joinder is impracticable. Upon information and belief, Plaintiffs allege that the Class contains many thousands of members. Although the precise number of Class members is unknown to Plaintiffs, the true number of Class members is known by Defendant, and thus, may be notified of the pendency of this action by first class mail, electronic mail, and/or published notice.

73. ***Existence and predominance of common questions of law and fact.*** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, but are not limited to, the following:

(a) whether Defendant collected, captured, received, or otherwise obtained biometric identifiers or biometric information from Plaintiffs and the Class;

(b) whether Defendant developed and made public its retention and deletion plan with for Plaintiffs' and Class Members' biometric data pursuant to §15(a) of the BIPA;

(c) whether Defendant destroyed Plaintiffs' and Class Members' biometrics when the purpose for collecting and obtaining them has been satisfied or within three years of Plaintiffs' and Class Members' use of the app;

(d) whether Defendant informed Plaintiffs and the Class before collecting, using, and storing their biometric identifiers or biometric information, as required by §15(b) the BIPA;

(e) whether Defendant informed Plaintiffs and the Class of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored and used, as required by §15(b) of the BIPA;

(f) whether Defendant obtained a written release, as defined by the BIPA, from Plaintiffs and the Class to collect, store, and use their biometric identifiers or biometric information;

(g) whether Defendant used biometric data to identify Plaintiffs and the Class;

(h) whether Defendant sold, leased, traded, or otherwise profited from Plaintiffs or Class Members' biometric identifiers and biometric information in violation of §15(c) of the BIPA;

(i) whether Defendant disclosed, redisclosed, or otherwise disseminated Plaintiffs and Class Members' biometric identifiers or biometric information in violation of §15(d) of the BIPA;

(j) whether Defendant protected Plaintiffs and Class Members' biometric identifiers or biometric information from disclosure as required by §15(e) of the BIPA;

(k) whether Defendant's violations of the BIPA were committed intentionally, recklessly or negligently;

(l) whether Plaintiffs and the Class are entitled to statutory damages under the BIPA and the correct measure of those damages; and

(m) whether Plaintiffs and the Class are entitled to declaratory and injunctive relief.

74. ***Typicality.*** Plaintiffs' claims are typical of the claims of the other members of the Class in that Defendant collected, stored, and used their biometrics without informed consent in the exact same manner as every other Class member.

75. ***Adequacy of representation.*** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel highly experienced in complex consumer class action litigation, and Plaintiffs intend to vigorously prosecute this action. Further, Plaintiffs have no interests that are antagonistic to those of the Class.

76. ***Superiority.*** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also

increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

77. The Class may also be certified because:

(a) the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for Defendant;

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

COUNT I

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule (On Behalf of Plaintiffs and the Class)

78. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

79. The BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Section 15 (a) of the BIPA requires that "[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

80. Facebook fails to comply with these BIPA mandates.

81. Facebook is a private entity under the BIPA. *See* 740 ILCS 14/10.

82. Plaintiffs and Class members are individuals under the BIPA (*see id*.) who have had their "biometric identifiers" collected as explained herein.

83. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by the BIPA. *See id.*

84. As alleged herein, Facebook collects, and is in possession of, biometric identifiers.

85. Facebook did not provide to Plaintiffs and putative Class Members a publicly available retention schedule or guidelines for permanently destroying users' biometric identifiers and information when the initial purpose for collecting such identifiers and information was satisfied or within 3 years of Plaintiffs' and Class members' last interactions with Facebook, as required by BIPA. Thus, Facebook violated Section 15(a) of the BIPA. Facebook's violations actually harmed or posed a material risk of harm to the privacy interests that BIPA seeks to protect.

86. Upon information and belief, Facebook lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and has not and will not destroy Plaintiffs' or the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the app.

87. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

88. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class members have suffered and will continue to suffer injury.

89. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS §

14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

COUNT II

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information (On Behalf of Plaintiffs and the Class)

90. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

91. Section 15(b) of the BIPA provides that a private entity may not, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .

740 ILCS 14/15(b).

92. Facebook is a private entity under the BIPA. *See* 740 ILCS 14/10.

93. Plaintiffs and the Class members are individuals under the BIPA. *See id*.

94. Facebook collected Plaintiffs and the Class members' biometric information and biometric identifiers as alleged above. *See id*.

95. Facebook systematically collected, used, and stored Plaintiffs and the Class members' biometric identifiers and biometric information without first obtaining the written release required by §15(b) of the BIPA.

96. As alleged above, Facebook did not inform Plaintiffs or the Class members in writing that their biometric identifiers or biometric information were being collected, stored and used, as required by §15(b) of the BIPA.

97. As alleged above, Facebook did not inform Plaintiffs or the Class members in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored and used, as required by §15(b) of the BIPA.

98. By collecting, storing, and using Plaintiffs and the Class members' biometric identifiers and biometric information as described herein, Facebook violated Plaintiffs and the Class members' rights to privacy in their biometric identifiers or biometric information, as set forth in the BIPA, 740 ILCS 14/1, *et seq*.

99. Facebook's violations of §15(b) of the BIPA were intentional or reckless because Facebook collected biometric data by default and without written notice as required by the BIPA and, therefore, Plaintiffs and the Class members had no opportunity to provide Defendant with a written release, as mandated by the BIPA. Alternatively, Facebook's violations of §15(b) of the BIPA were negligent because Facebook failed to meet the applicable standard of care in ensuring that its members were informed and consented to the collection, storage, and use of their biometric information and biometric identifiers.

100. As a result of Defendant's violations of §15(b) of the BIPA, Plaintiffs seek the following relief individually and on behalf of the Class: (l) injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring Facebook to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as alleged herein; (2) statutory damages of $5,000 for each intentional or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees, costs, and expenses pursuant to 740 ILCS 14/20(3).

COUNT III

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c): Profits Unlawfully Derived From Biometric Identifiers and Biometric Information (On Behalf of Plaintiffs and the Class)

101. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

102. Section 15(c) of the BIPA provides "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."

103. As alleged above, Facebook violated the BIPA by unlawfully profiting from individuals' biometric identifiers and biometric information, including the biometric identifiers and information of Plaintiffs and Class members.

104. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

105. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class members have suffered and will continue to suffer injury.

106. Plaintiffs and Class members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

107. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs and Class members' biometric identifiers and information.

108. Plaintiffs and Class members also seek punitive damages, injunctive relief, and the reasonable attorneys' fees, costs, and expenses relating to this action.

COUNT IV

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent (On Behalf of Plaintiffs and the Class)

109. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

110. Section 15(d) of the BIPA provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information [...]."

111. As alleged above, Facebook violated the BIPA by disclosing and otherwise disseminating, upon information and belief, individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiffs and Class members, even though: (a) neither the subjects of the biometric identifiers and information, nor their authorized representatives, consented to the disclosure; (b) the disclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure was not required by state or federal law or municipal ordinance; and (d) the disclosure and redisclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

112. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

113. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class members have suffered and will continue to suffer injury.

114. Plaintiffs and Class members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

115. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs and Class members' biometric identifiers and information.

116. Plaintiffs and Class members also seek punitive damages, injunctive relief, and the reasonable attorney fees, costs, and expenses relating to this action.

COUNT V

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(e): Failure to Protect Biometric Identifiers and Biometric Information From Disclosure (On Behalf of Plaintiffs and the Class)

117. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

118. Section 15(e) of the BIPA provides that "[a] private entity in possession of a biometric identifier or biometric information shall:"

> (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
>
> (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

119. As alleged above, upon information and belief, Facebook violated the BIPA because, while in possession of Plaintiffs and Class members' biometric identifiers and information, it failed to protect from disclosure those biometric identifiers and information: (a) using the reasonable standard of care within Facebook industry; and (b) in a manner that is the same as or more protective than the manner in which Facebook protects and protected other confidential and sensitive information when it voluntarily disclosed the biometrics to third parties.

120. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

121. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class members have suffered and will continue to suffer injury.

122. Plaintiffs and Class members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

123. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs and Class members' biometric identifiers and information.

124. Plaintiffs and Class members also seek punitive damages, injunctive relief, and the reasonable attorneys' fees, costs, and expenses relating to this action.

COUNT VI

Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

125. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

126. Facebook obtained a monetary benefit from Plaintiffs and Class members to their detriment. Facebook did so by profiting off of the covert and unauthorized collection of the biometric identifiers and information of Plaintiffs and Class members, while exposing Plaintiffs and Class members to a heightened risk of privacy harms and depriving them of their control over their biometric data.

127. Plaintiffs and Class members did not authorize Facebook to collect, capture, obtain, disclose, redisclose, disseminate and otherwise profit off from their biometric identifiers and information.

128. Facebook appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Facebook's conduct toward Plaintiffs and Class members as described herein.

129. Facebook sold, leased, traded, and/or otherwise profited from Plaintiffs and Class members' biometric identifiers and information and did not provide full compensation for the benefit received from Plaintiffs and Class members.

130. Facebook acquired and caused to be acquired Plaintiffs and Class members' biometric identifiers and information through inequitable means in that it collected, captured, and otherwise obtained biometric data from Plaintiffs and Class members' online photos without permission and in violation of Illinois law.

131. Plaintiffs and Class members have no adequate remedy at law.

132. Under the circumstances, it would be unjust and unfair for Facebook to be permitted to retain any of the benefits obtained from Plaintiffs and Class members and their biometric identifiers and information.

133. Under the principles of equity and good conscience, Facebook should not be permitted to retain the biometric identifiers and information belonging to Plaintiffs and Class members because Facebook unlawfully obtained the biometric identifiers and information.

134. Facebook should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, redisclosure, dissemination, and profiting from Plaintiffs and Class members' biometric identifiers and information, including, but not limited to, the value of the intellectual property derived therefrom.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for a judgment against Defendant as follows:

A. Certifying the Class as defined above, appointing Plaintiffs as Class Representatives, and appointing their undersigned counsel as Class counsel;

B. Declaring that Defendant's actions, as alleged above, violate Sections 15 (a), (b),(c),(d), and (e) of the BIPA, 740 ILCS 14/1, *et seq*.;

C. Awarding statutory damages of $5,000 for each intentional or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1);

D. Awarding injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring Facebook to comply with the BIPA by providing a publicly available retention schedule or guidelines for permanently destroying its users' biometric identifiers and biometric information and forcing Defendant to stop collecting, storing, and using Plaintiffs and the Class members' biometric identifiers and biometric information without first obtaining their informed written consent;

E. An order requiring Facebook to disgorge into a common fund or constructive fund, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, dissemination, and profiting from Plaintiffs and Class members' biometric identifiers and information;

F. An award of pre-judgment and post-judgment interest for Plaintiffs and Class members, as permitted by law;

G. Awarding Plaintiffs attorneys' fees and costs pursuant to 740 ILCS 14/20(3); and

H. Awarding any further relief as the Court may deem just and proper.

VII. JURY DEMAND

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: January 26, 2021

CARLSON LYNCH LLP

By: */s/Todd D. Carpenter*

Todd D. Carpenter (234464)
1350 Columbia St., Ste. 603
San Diego, CA 92101
Tel.: (619) 762-1900
Fax: (619) 756-6991
tcarpenter@carlsonlynch.com

Kyle A. Shamberg*
Nicholas R. Lange*
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, IL 60602
Tel.: (312) 750-1265
kshamberg@carlsonlynch.com
nlange@carlsonlynch.com

Matthew E. Lee*
Erin J. Ruben*
WHITFIELD BRYSON LLP
900 W. Morgan Street
Raleigh, North Carolina 27603
Tel.: (919) 600-5000
Fax: (919) 600-5035
dan@whitfieldbryson.com
matt@whitfieldbryson.com
erin@whitfieldbryson.com

Gregory F. Coleman*
Lisa A. White*
Jonathan B. Cohen
GREG COLEMAN LAW PC
800 Gay Street, Suite 1100
Knoxville, TN 37929
Tel.: (865) 247-0080
Fax: (865) 522-0049
greg@gregcolemanlaw.com
lisa@gregcolemanlaw.com
jonathan@gregcolemanlaw.com

*Pro Hac Vice applications pending

Counsel for Plaintiffs and the Proposed Class